PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L 9/08	A1	(11) Numéro de publication internationale: **WO 00/56006**
		(43) Date de publication internationale: 21 septembre 2000 (21.09.00)

(21) Numéro de la demande internationale: PCT/FR00/00680

(22) Date de dépôt international: 17 mars 2000 (17.03.00)

(30) Données relatives à la priorité:
99/03329 17 mars 1999 (17.03.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: SCHLUMBERGER SYSTEMES [FR/FR]; 50, avenue Jean Jaurès, F–92120 Montrouge (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: DOLLET, Richard [FR/FR]; 15, rue Poirier de Narçay, F–75014 Paris (FR).

(74) Mandataire: UTZMANN–NORTH, Anne; Schlumberger Systemes, Test & Transactions, 50, avenue Jean Jaurès, Boîte Postale 620–12, F–92542 Montrouge Cedex (FR).

(81) Etats désignés: CN, MX, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: SECURE METHOD FOR LOADING DATA BETWEEN SECURITY MODULES

(54) Titre: PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE

(57) Abstract

The invention concerns a secure method for loading secret data from a first security module towards a second security module, said first module comprising secret data, said second module comprising a first non–volatile memory and a second volatile memory. The invention is characterised in that said method comprises steps which consist in: recording data comprising random data in the first memory of the second module; sending to the second module secret data from the first module encrypted from the random data; transferring the data comprising the random data from the first memory to the second memory of the second module; decrypting said encrypted secret data, from the random data; and recording, in the second memory, said decrypted secret data. The invention is particularly applicable to telephone systems.

(57) Abrégé

L'invention concerne un procédé de chargement sécurisé de données secrètes à partir d'un premier module de sécurité vers un deuxième module de sécurité, ledit premier module comportant des données secrètes, ledit deuxième module comportant une première mémoire non volatile et une deuxième mémoire volatile. L'invention se caractérise en ce que ledit procédé comporte des étapes selon lesquelles, on enregistre des informations comprenant une donnée aléatoire dans la première mémoire du deuxième module, on envoie au deuxième module une donnée secrète du premier module chiffrée à partir de la donnée aléatoire, on transfère les informations comprenant la donnée aléatoire de la première mémoire vers la deuxième mémoire du deuxième module, on déchiffre ladite donnée secrète chiffrée, à partir de la donnée aléatoire, et, on enregistre, dans le deuxième module, ladite donnée secrète déchiffrée. L'invention s'applique, en particulier, à la téléphonie.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE

La présente invention concerne un procédé de chargement sécurisé de données secrètes à partir d'un premier module de sécurité vers au moins un deuxième module de sécurité, ledit premier module comportant au moins un fichier de données secrètes, ledit deuxième module comportant une première mémoire non volatile et une deuxième mémoire volatile.

L'invention trouve une application particulièrement avantageuse dans le domaine de la téléphonie.

Dans le domaine de la téléphonie, il existe des systèmes d'administration de terminaux qui comportent un premier module de sécurité embarqué dans un serveur d'administration et des deuxièmes modules de sécurité généralement embarqués dans les terminaux précités. Les terminaux sont appelés publiphones.

Un deuxième module de sécurité garantit la validité d'une carte utilisateur introduite dans un publiphone, notamment grâce à une authentification de ladite carte. A cet effet, ledit deuxième module de sécurité comprend dans sa première mémoire des données secrètes permettant de garantir ladite validité des cartes utilisateurs. Les systèmes d'administration de publiphones ainsi que les données secrètes sont gérés par des opérateurs de téléphonie. Afin de diminuer les risques de fraude consistant à espionner un réseau de communication reliant le serveur et les publiphones et ainsi à découvrir lesdites données secrètes, les opérateurs sont amenés à modifier régulièrement tout ou partie des données secrètes d'un deuxième module de sécurité d'un publiphone, à partir de données secrètes contenues dans un fichier du premier module de sécurité.

Un procédé connu de la technique comprend les étapes selon lesquelles :

- on chiffre les données secrètes du premier module de sécurité qui doivent être transmises au deuxième module de sécurité et qui se trouvent dans le serveur d'administration,
- le publiphone se connecte au serveur d'administration lorsqu'aucune conversation n'est en cours,
- les données secrètes sont transmises au deuxième module de sécurité se trouvant dans le publiphone.

Lorsque le publiphone se connecte au serveur d'administration, il est indisponible à tout utilisateur, ainsi la connexion se fait généralement la nuit. L'échange de données se fait en mode déconnecté appelé dans le langage anglo-saxon mode "off-line".

Afin de diversifier les transmissions de données secrètes, on fait intervenir une donnée pseudo-aléatoire basée sur une valeur d'un compteur contenu dans le deuxième module de sécurité. A chaque échange de données secrètes, la valeur du compteur est incrémentée, le premier module de sécurité doit connaître la valeur dudit compteur et incrémenter un compteur local dédié audit deuxième module.

Bien que ce procédé permette un chargement de données secrètes entre un premier et deuxième modules de sécurité, il nécessite une administration lourde de bases de données permettant de garantir la synchronisation des différents compteurs. En effet, une trace de l'ensemble des échanges effectués avec un deuxième module de sécurité doit être conservée. De plus, ce procédé ne garantit pas un échange de données parfaitement diversifié.

Aussi, un problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de chargement sécurisé de données secrètes à partir d'un premier module de sécurité vers au moins un deuxième module de sécurité, ledit premier module comportant au moins un fichier de données secrètes, ledit deuxième module comportant une première mémoire non volatile et une deuxième

mémoire volatile, qui permettrait de garantir un échange de données parfaitement diversifié entre un premier et deuxième modules de sécurité, en mode "off-line", tout en évitant une gestion trop lourde de bases de données.

Une solution au problème technique posé se caractérise, selon l'invention, en ce que ledit procédé de chargement comporte les étapes selon lesquelles :

- on génère au moins une donnée aléatoire dans la deuxième mémoire du deuxième module,
- on enregistre des informations comprenant ladite donnée aléatoire dans la première mémoire du deuxième module,
- on envoie au premier module la donnée aléatoire,
- dans le premier module, on chiffre une donnée secrète du fichier dudit premier module, à partir de la donnée aléatoire et d'un algorithme de cryptage,
- on envoie au deuxième module ladite donnée secrète chiffrée,
- on transfère les informations, comprenant la donnée aléatoire de la première mémoire du deuxième module, de ladite première mémoire vers la deuxième mémoire dudit module,
- on déchiffre ladite donnée secrète chiffrée, à partir d'un algorithme de décryptage et de la donnée aléatoire, et, on enregistre dans le deuxième module, ladite donnée secrète déchiffrée.

Ainsi, comme on le verra en détail plus loin, le procédé de chargement de l'invention permet, en utilisant une donnée aléatoire pour le chargement des données secrètes, d'améliorer la sécurité du chargement des données en diversifiant de façon parfaite les données transmises. Ainsi, un fraudeur qui espionne un réseau de communication et récupère les données transmises n'obtient jamais une même valeur de chiffrement et ne peut par conséquent découvrir

un secret relatif aux données secrètes transmises. De plus, le fait d'enregistrer la donnée aléatoire dans une mémoire non volatile du deuxième module de sécurité permet de l'utiliser en mode "off-line", puisque ladite donnée aléatoire n'est pas perdue lorsque ledit deuxième module de sécurité est mis hors tension.

La description qui va suivre au regard des dessins annexés, donnée à titre d'exemple non limitatif, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est un schéma montrant un premier module de sécurité et plusieurs deuxièmes modules de sécurité.

La figure 2 est un schéma montrant le premier module et un deuxième module de la figure 1.

La figure 3 est un schéma montrant un échange de données entre le premier module et le deuxième module de la figure 2.

La figure 4 un schéma montrant un deuxième échange de données entre le premier module et le deuxième module de la figure 2.

La figure 5 un schéma montrant un troisième échange de données entre le premier module et le deuxième module de la figure 2.

Sur la figure 1 est représenté un premier module S de sécurité et plusieurs deuxièmes modules SAM de sécurité, chaque deuxième module SAM comprenant une première mémoire M1 non volatile et une deuxième mémoire M2 volatile appelée mémoire de travail. La figure 2 montre le premier module S et un deuxième module SAM. Le premier module S comporte au moins un fichier EF1 de données secrètes DATA et un algorithme ALGO de cryptage. Un fichier de données secrètes est généralement associé à un opérateur de téléphonie donné. Le deuxième module SAM comporte un algorithme ALGOP de décryptage inverse de l'algorithme ALGO de cryptage et des données secrètes DATA.

Afin de modifier une donnée secrète du deuxième module SAM, il faut charger une donnée secrète à partir du fichier EF1 du premier

module S de sécurité. Le chargement doit se faire de façon sécurisée. La donnée secrète est ainsi transmise de manière chiffrée. La phase de chargement comprend plusieurs étapes décrites ci-après.

Dans une première étape, on génère au moins une donnée aléatoire RAND dans la mémoire M2 volatile du deuxième module SAM.

Dans une deuxième étape, comme le montre la figure 3, on enregistre des informations INFO comprenant ladite donnée aléatoire RAND dans la mémoire M1 non volatile du deuxième module SAM. Un emplacement mémoire dans ladite mémoire M1 non volatile est réservé à cet effet et est initialisé par défaut à une valeur d'initialisation V.

Dans un premier mode de réalisation, les informations INFO, comprenant ladite donnée aléatoire RAND, comportent un indice relatif à une donnée secrète DATA. L'indice étant par exemple un numéro de donnée secrète à modifier ou un indice d'emplacement mémoire dans lequel une donnée secrète doit être chargée dans le deuxième module SAM. Ainsi, dans le cas où le deuxième module SAM est mis hors tension pour des raisons d'économie d'énergie, la donnée aléatoire RAND et les informations associées ne sont pas perdues.

Dans une troisième étape, on envoie au premier module S la donnée aléatoire RAND. On notera que la deuxième et la troisième étape peuvent être permutées.

Afin de réduire le nombre d'accès au deuxième module SAM, la génération et l'envoi de la donnée aléatoire RAND ainsi que l'enregistrement des informations INFO dans le deuxième module SAM, se font au moyen d'une première commande ASKLOADING. Cette première commande est envoyée par le serveur d'administration au deuxième module SAM via le publiphone (non représenté).

Dans une quatrième étape, dans le premier module S, on chiffre la donnée secrète DATA du fichier EF1 qui doit être transmise dans le deuxième module SAM. Le chiffrement comprend une étape de cryptage

utilisant l'algorithme ALGO de cryptage et la donnée aléatoire RAND. L'utilisation de la donnée aléatoire RAND évite d'avoir une même valeur de chiffrement pour une donnée secrète DATA. Ainsi, un fraudeur pourra difficilement faire un lien entre les différentes données transmises sur le réseau de communication, celles-ci étant différentes à chaque transmission. Le chiffrement peut également comprendre, d'une part, une étape de signature de la donnée secrète DATA basée sur la donnée aléatoire RAND, et, d'autre part, une étape de certification des données transmises. La signature permet de vérifier l'authenticité de la donnée secrète DATA chargée et le certificat permet de vérifier l'intégrité des données transmises.

Dans une cinquième étape, comme le montre la figure 4, on envoie au deuxième module SAM ladite donnée secrète chiffrée DATAC.

Dans une sixième étape, on transfère les informations INFO, comprenant la donnée aléatoire RAND de la mémoire M1 non volatile du deuxième module SAM, de ladite mémoire M1 vers la mémoire M2 de travail dudit module SAM. Ainsi, on récupère dans la mémoire M2 de travail, la donnée aléatoire RAND, qui a été utilisée pour chiffrer la donnée secrète DATA, ainsi que les informations associées.

La duplication de la donnée aléatoire RAND et des informations associées dans deux mémoires différentes du deuxième module SAM peut générer des incohérences dans ledit module et des problèmes de sécurité. Aussi, on ne garde qu'un seul jeu d'informations INFO dans le deuxième module SAM. A cet effet, postérieurement à l'enregistrement des informations INFO comprenant ladite donnée aléatoire RAND dans la première mémoire M1 du deuxième module SAM (figure 3), on efface les informations INFO se trouvant dans la deuxième mémoire M2 dudit deuxième module SAM. De la même manière, postérieurement au transfert des informations INFO comprenant la donnée aléatoire RAND, de la première mémoire M1 du deuxième module SAM dans la deuxième

mémoire M2 dudit module (figure 4), on efface lesdites informations INFO dans ladite première mémoire M1.

Enfin, dans une dernière étape, on déchiffre ladite donnée secrète chiffrée DATAC, à partir de l'algorithme ALGOP de décryptage du deuxième module SAM et de la donnée aléatoire RAND, et, on enregistre dans le deuxième module SAM ladite donnée secrète DATA déchiffrée.

Afin de réduire le nombre d'accès au deuxième module SAM, le transfert des informations INFO, le déchiffrement de la donnée secrète DATA dans le deuxième module SAM et l'enregistrement, se font au moyen d'une deuxième commande ADMINRECOVER. Cette deuxième commande est envoyée par le serveur d'administration au deuxième module SAM via le publiphone (non représenté). Dans le cas où un incident survient lors du chargement, ou à la fin dudit chargement, l'emplacement mémoire, dans la mémoire M1 non volatile, où se trouvent les informations INFO comprenant la donnée aléatoire RAND, est réinitialisé à la valeur d'initialisation V . Si un incident est survenu, une autre donnée aléatoire RAND est générée et les différentes étapes du procédé décrites ci-dessus sont effectuées de nouveau. Lorsque la deuxième commande ADMINRECOVER est envoyée, on vérifie qu'une donnée aléatoire RAND a été générée et enregistrée. Ainsi, on vérifie que l'emplacement mémoire de la première mémoire M1 non volatile du deuxième module SAM, réservé à la donnée aléatoire RAND, ne comporte pas la valeur d'initialisation V. Si tel est le cas, la deuxième commande ADMINRECOVER est exécutée. Dans le cas contraire, elle n'est pas exécutée et on effectue la première étape du procédé.

Généralement, un deuxième module SAM gère différents types de carte utilisateur et comporte par suite plusieurs données secrètes DATA associées à chaque type de carte utilisateur, un type de carte correspondant communément à un opérateur donné, fournisseur desdites cartes. Il est habituel de vouloir modifier l'ensemble des

données secrètes DATA associées à un type de cartes. Dans ce cas, on effectue les premières étapes du procédé de l'invention comme décrit précédemment, mais en les appliquant à l'ensemble des données secrètes DATA à modifier. Ainsi, on génère successivement plusieurs données aléatoires RAND dans la deuxième mémoire M2 du deuxième module SAM et on enregistre dans la première mémoire M1 du deuxième module SAM, consécutivement à chaque génération de donnée aléatoire RAND, les informations INFO comprenant la donnée aléatoire RAND générée. Comme le montre l'exemple de la figure 5, on génère trois données aléatoires RAND1, RAND2 et RAND3 dans le deuxième module SAM et on les enregistre dans la mémoire M1 non volatile dudit module. Par la suite, on envoie les trois données aléatoires générées au premier module S du serveur d'administration. On chiffre trois données secrètes DATA1, DATA2 et DATA3 se trouvant dans le fichier EF1 du premier module S et correspondant aux trois données secrètes à modifier dans le deuxième module SAM. La correspondance est effectuée grâce par exemple à trois indices (1,2 et 3) de donnée secrète envoyés en même temps que les trois données aléatoires RAND. Enfin, pour transmettre les trois données secrètes DATA1, DATA2 et DATA3 dans ledit deuxième module SAM, on effectue toutes les étapes du procédé de l'invention comme décrit précédemment, à partir de la cinquième étape pour chaque donnée secrète DATA à charger ou pour l'ensemble des données secrètes DATA comme avec les précédentes étapes.

Ainsi, suivant un premier mode de réalisation du chargement de plusieurs données décrit ci-dessus, lors de chaque chargement, on utilise une donnée aléatoire RAND pour charger une donnée secrète DATA. Suivant un second mode de réalisation, afin de diminuer le temps de chargement des données secrètes, lors de chaque chargement,

on utilise une unique donnée aléatoire RAND pour charger plusieurs données secrètes DATA.

Bien entendu, l'invention n'est nullement limitée au domaine de la téléphonie, elle peut s'étendre à d'autres domaines dans lesquels est mis en oeuvre un système d'échange de données entre un module centralisé disposant de données secrètes et des modules délocalisés aptes à recevoir lesdites données secrètes.

REVENDICATIONS

1 - Procédé de chargement sécurisé de données secrètes à partir d'un premier module (S) de sécurité vers au moins un deuxième module (SAM) de sécurité, ledit premier module (S) comportant au moins un fichier (EF1) de données secrètes (DATA), ledit deuxième module (SAM) comportant une première mémoire (M1) non volatile et une deuxième mémoire (M2) volatile, caractérisé en ce qu'il comporte les étapes selon lesquelles :

- on génère au moins une donnée aléatoire (RAND) dans la deuxième mémoire (M2) du deuxième module (SAM),
- on enregistre des informations (INFO) comprenant ladite donnée aléatoire (RAND) dans la première mémoire (M1) du deuxième module (SAM),
- on envoie au premier module (S) la donnée aléatoire (RAND),
- dans le premier module (S), on chiffre une donnée secrète (DATA) du fichier (EF1) dudit premier module (S), à partir de la donnée aléatoire (RAND) et d'un algorithme (ALGO) de cryptage,
- on envoie au deuxième module (SAM) ladite donnée secrète chiffrée (DATAC),
- on transfère les informations (INFO), comprenant la donnée aléatoire (RAND) de la première mémoire (M1) du deuxième module (SAM), de ladite première mémoire (M1) vers la deuxième mémoire (M2) dudit module (SAM),
- on déchiffre ladite donnée secrète chiffrée (DATAC), à partir d'un algorithme (ALGOP) de décryptage et de la donnée aléatoire (RAND), et, on enregistre dans le deuxième module (SAM), ladite donnée secrète (DATA) déchiffrée.

2 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- postérieurement à l'enregistrement des informations (INFO) comprenant ladite donnée aléatoire (RAND) dans la première mémoire (M1) du deuxième module (SAM), on efface les informations (INFO) se trouvant dans la deuxième mémoire (M2) dudit deuxième module (SAM).

3 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- postérieurement au transfert des informations (INFO) comprenant la donnée aléatoire (RAND), de la première mémoire (M1) du deuxième module (SAM) dans la deuxième mémoire (M2) dudit module, on efface lesdites informations (INFO) dans ladite première mémoire (M1).

4 - Procédé selon l'une des revendications précédentes, caractérisé en ce que la génération et l'envoi de la donnée aléatoire (RAND) ainsi que l'enregistrement des informations (INFO) dans le deuxième module (SAM), se font au moyen d'une première commande (ASKLOADING).

5 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le transfert des informations (INFO), le déchiffrement de la donnée secrète (DATA) dans le deuxième module (SAM) et l'enregistrement, se font au moyen d'une deuxième commande (ADMINRECOVER).

6 - Procédé selon l'une des revendications précédentes, caractérisé en ce que les informations (INFO), comprenant ladite donnée aléatoire (RAND), comportent un indice relatif à une donnée secrète (DATA).

7 - Procédé selon l'une des revendications précédentes, caractérisé en ce que l'on génère successivement plusieurs données aléatoires (RAND) dans la deuxième mémoire (M2) du deuxième module (SAM) et on enregistre dans la première mémoire (M1) du deuxième module (SAM), consécutivement à chaque génération de donnée aléatoire (RAND), les informations (INFO) comprenant la donnée aléatoire (RAND) générée.

8 - Procédé selon l'une des revendications précédentes, caractérisé en ce que, lors de chaque chargement, on utilise une donnée aléatoire RAND pour charger une donnée secrète DATA.

9 - Procédé selon l'une des revendications 1 à 7, caractérisé en ce que, lors de chaque chargement, on utilise une unique donnée aléatoire RAND pour charger plusieurs données secrètes DATA.

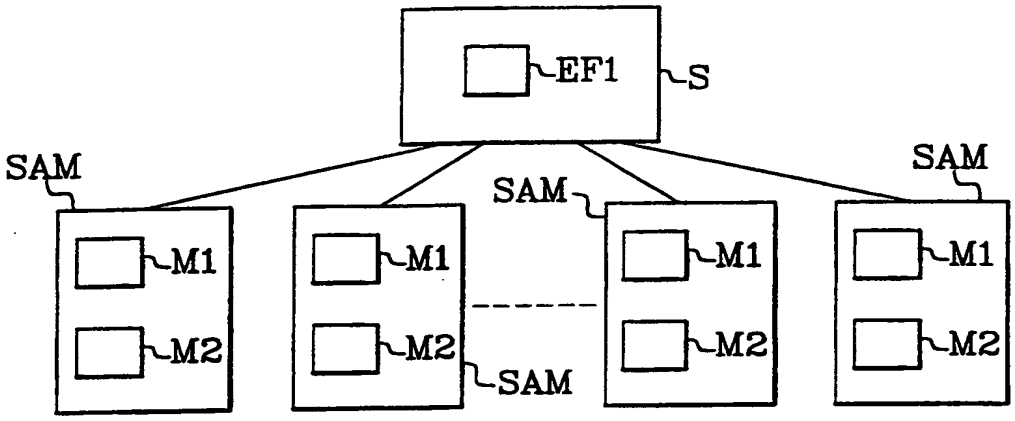

FIG.1

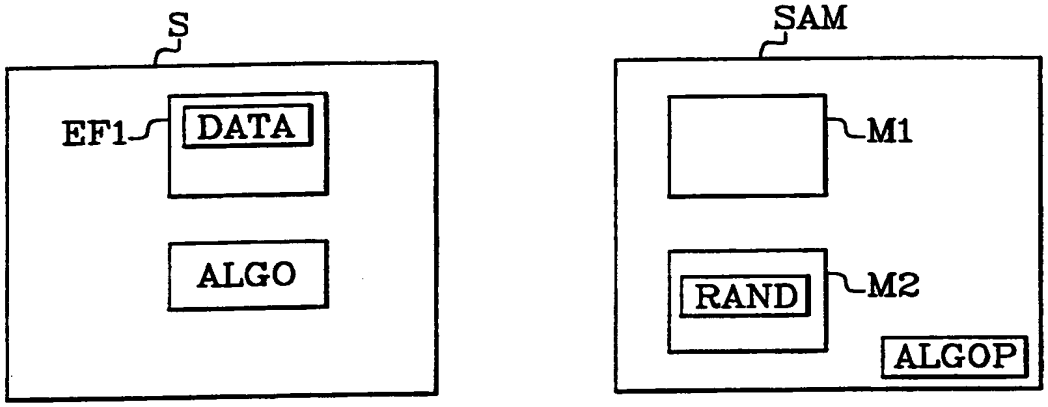

FIG.2

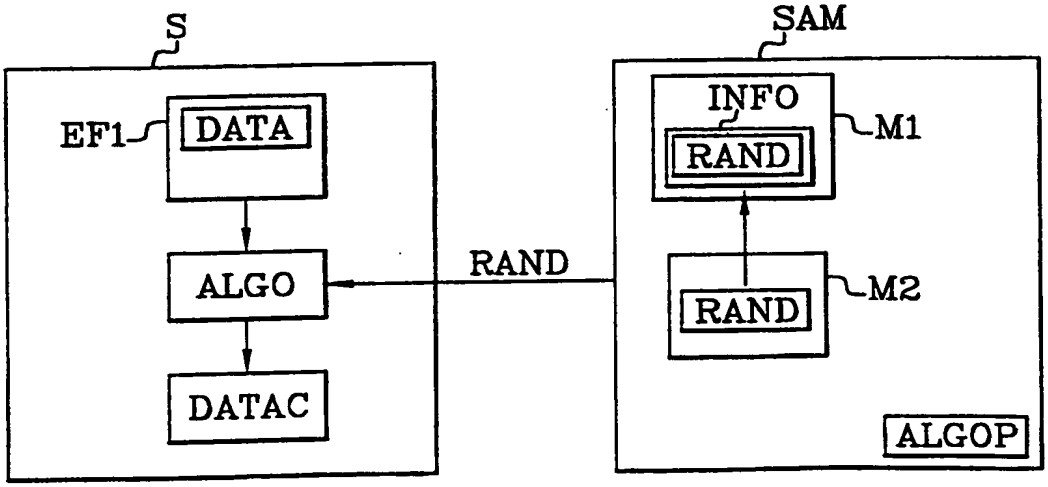

FIG.3

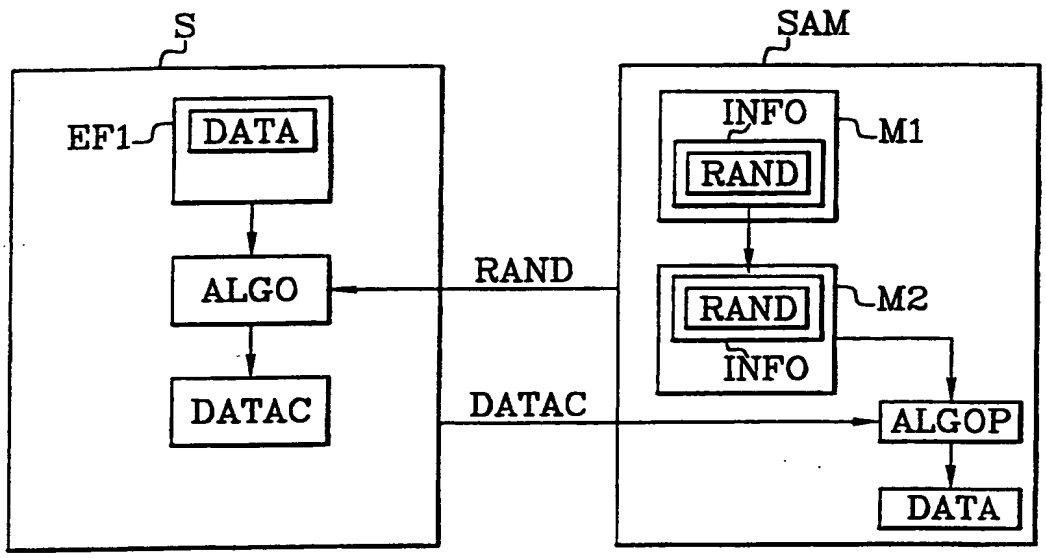
S
SAM
EF1
DATA
ALGO
DATAC
RAND
DATAC
INFO
RAND
M1
RAND
INFO
M2
ALGOP
DATA

FIG.4

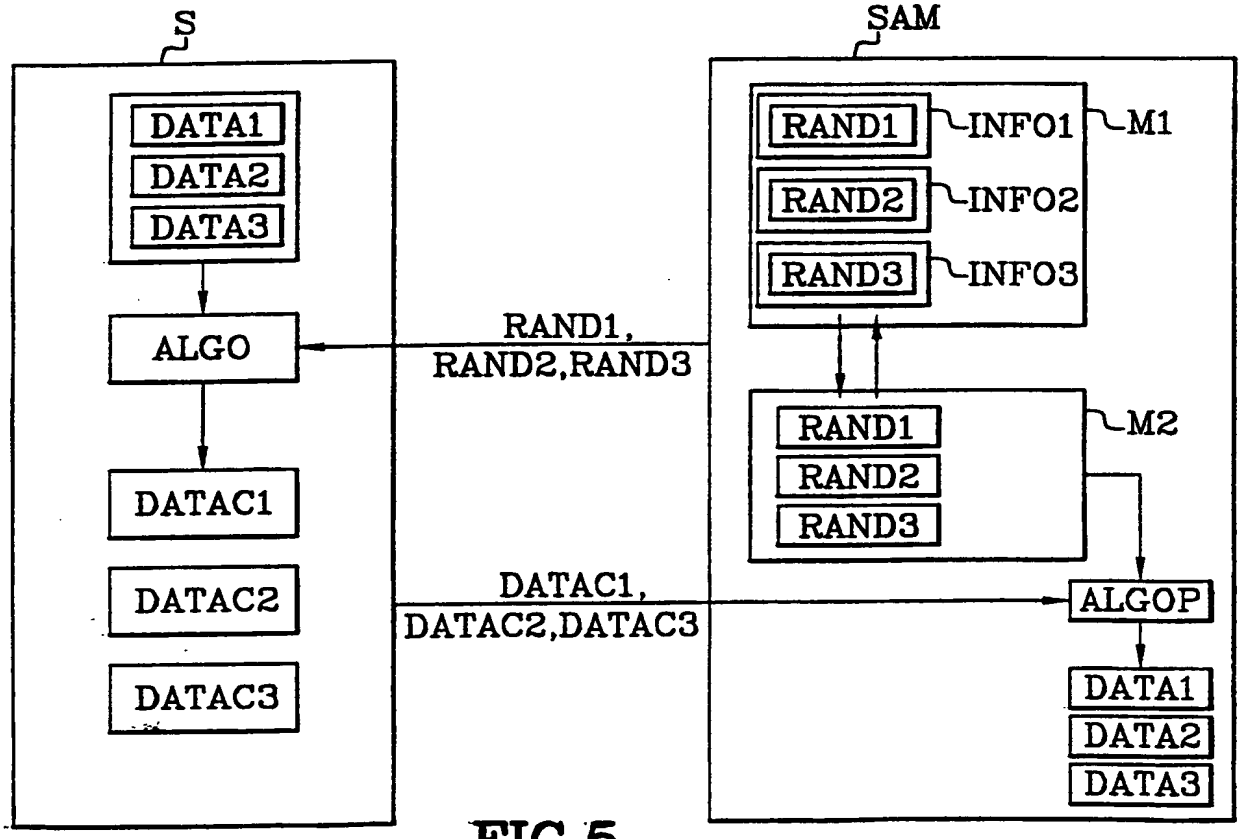
S
SAM
DATA1
DATA2
DATA3
ALGO
DATAC1
DATAC2
DATAC3
RAND1,
RAND2,RAND3
DATAC1,
DATAC2,DATAC3
RAND1
RAND2
RAND3
INFO1
INFO2
INFO3
M1
RAND1
RAND2
RAND3
M2
ALGOP
DATA1
DATA2
DATA3

FIG.5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 00/00680

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 517 567 A (EPSTEIN PHILIP) 14 May 1996 (1996-05-14) abstract column 3, line 52 -column 4, line 35 column 5, line 55 -column 7, line 40 column 8, line 5 - line 10	1-3,6,8, 9
A	US 4 731 840 A (MNISZEWSKI SUSAN M ET AL) 15 March 1988 (1988-03-15) abstract column 2, line 34 -column 3, line 25 claim 1	1-9
A	FR 2 681 165 A (GEMPLUS CARD INT) 12 March 1993 (1993-03-12) abstract page 5, line 17 - line 30 page 7, line 20 -page 10, line 18	1-9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 May 2000	06/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 00/00680

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5517567 A	14-05-1996	NONE	
US 4731840 A	15-03-1988	NONE	
FR 2681165 A	12-03-1993	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 00/00680

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 5 517 567 A (EPSTEIN PHILIP) 14 mai 1996 (1996-05-14) abrégé colonne 3, ligne 52 -colonne 4, ligne 35 colonne 5, ligne 55 -colonne 7, ligne 40 colonne 8, ligne 5 - ligne 10	1-3,6,8, 9
A	US 4 731 840 A (MNISZEWSKI SUSAN M ET AL) 15 mars 1988 (1988-03-15) abrégé colonne 2, ligne 34 -colonne 3, ligne 25 revendication 1	1-9
A	FR 2 681 165 A (GEMPLUS CARD INT) 12 mars 1993 (1993-03-12) abrégé page 5, ligne 17 - ligne 30 page 7, ligne 20 -page 10, ligne 18	1-9

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
29 mai 2000	06/06/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Gautier, L

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 00/00680

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5517567 A	14-05-1996	AUCUN	
US 4731840 A	15-03-1988	AUCUN	
FR 2681165 A	12-03-1993	AUCUN	

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 00/00680

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 517 567 A (EPSTEIN PHILIP) 14 May 1996 (1996-05-14) abstract column 3, line 52 -column 4, line 35 column 5, line 55 -column 7, line 40 column 8, line 5 - line 10	1-3,6,8, 9
A	US 4 731 840 A (MNISZEWSKI SUSAN M ET AL) 15 March 1988 (1988-03-15) abstract column 2, line 34 -column 3, line 25 claim 1	1-9
A	FR 2 681 165 A (GEMPLUS CARD INT) 12 March 1993 (1993-03-12) abstract page 5, line 17 - line 30 page 7, line 20 -page 10, line 18	1-9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 May 2000	06/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Gautier, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 00/00680

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5517567 A	14-05-1996	NONE	
US 4731840 A	15-03-1988	NONE	
FR 2681165 A	12-03-1993	NONE	